Mitigating the Threats for Digital Credentials API

Simone Onofri

TPAC 2024
Anaheim CA, USA
hybrid meeting
23–27 SEPTEMBER 2024

Agenda

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?
(metaphorical question)

#credentials-threats (thank you for scribing!)

This session is collaborative.
Use the QR code to access the slides and the interactive model
(you have to *trust* the QR Code link)

SCAN ME

What are we working on?

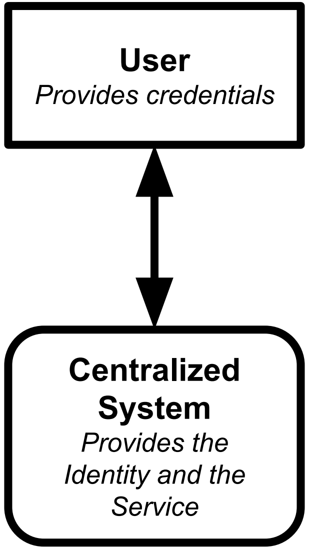
History

- For **centuries** there has been interest in **identities, and credentials** to "present" them.
- In recent **decades** there is the same interest in **bringing identity and credentials** to the **Internet** and the **Web**
- Starting from a **centralized** model, in **recent years**, interest has focused on the **federated** and **decentralized model**
- A long story of threats and mitigations...

What are we working on?

Centralized Model

- It is the centralized model, the credentials and the service are offered by the same provider.
- The **threats** are that the user has to **remember so many passwords**, **services have to store and protect so many passwords**, and there is a **risk of phishing**, and all is under the control of the centralized system....



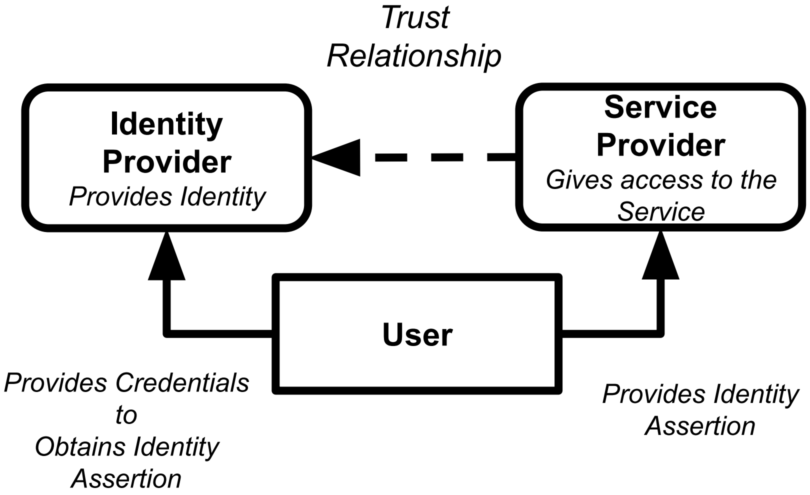
User
Provides credentials

Centralized System
Provides the Identity and the Service

What are we working on?

Federated Model

- In Federated Model, we have third-party services that we manage our identity (IdP) and use them to access various services.
- We **mitigated** the threat of **remembering so many passwords** and that not all **services have to protect passwords**
- But the **IdP has control over our identity** and can **track us** (and we depend on **third-party cookies**).
- We introduced **new elements** e.g., how do the various actors **trust** each other? It used to be much simpler in Centralized Model.

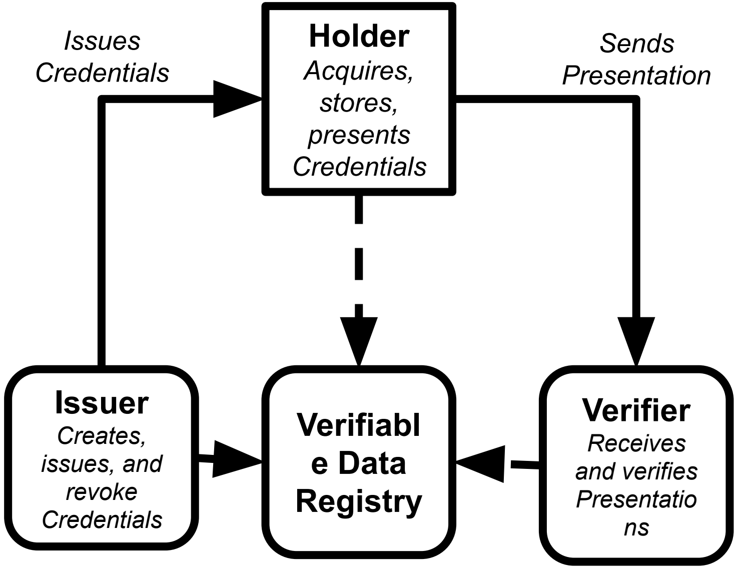


Trust Relationship
Identity Provider
Provides Identity
Service Provider
Gives access to the Service
User
Provides Credentials to Obtains Identity Assertion
Provides Identity Assertion

What are we working on?

Decentralized Model

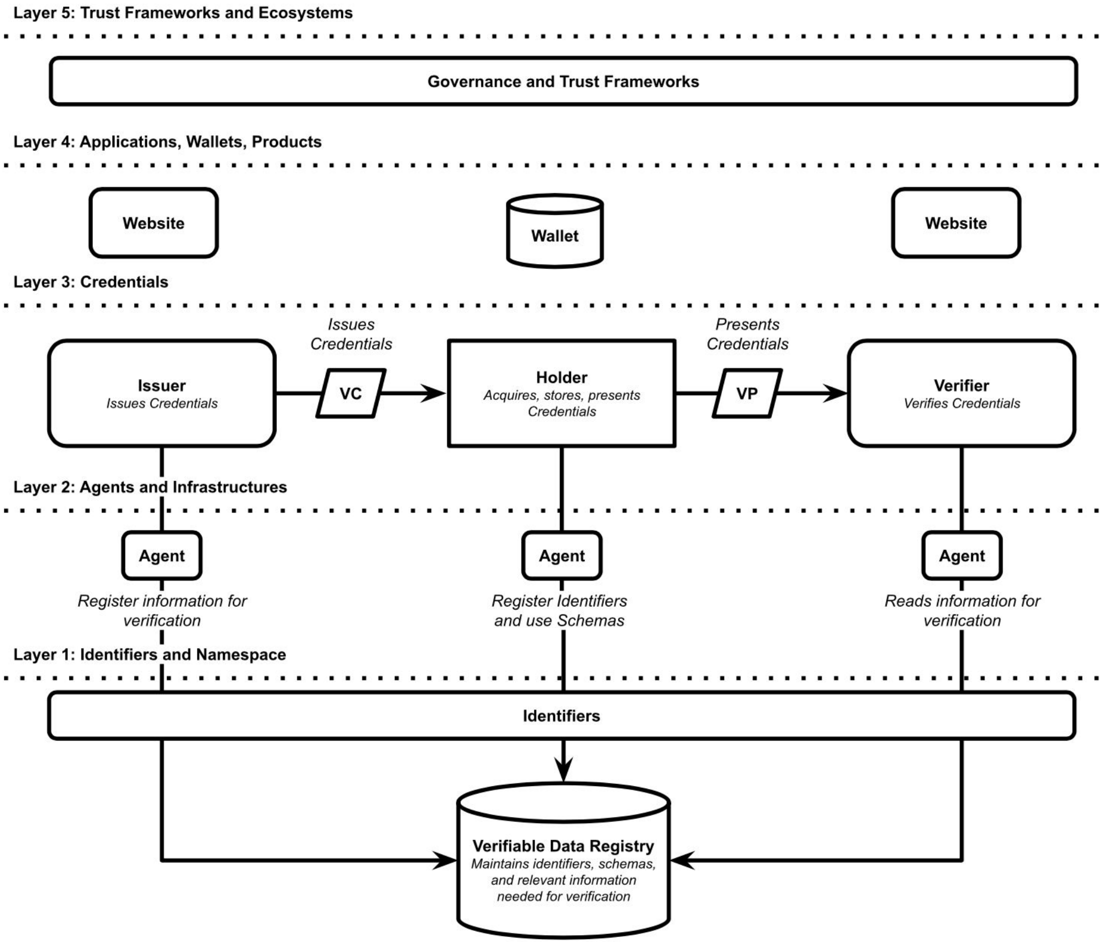
- In the Decentralized model, the user maintains credentials that are issued to him or her independently, without control of the issuer.
- So we have mitigated IdP tracking, increased user autonomy
- But we need new protocols and formats, we need **Wallets**, credentials status management, and more. Trust becomes an even bigger issue.
- This is normal, these are new challenges that we have to face (and mitigate).


Issues Credentials
Holder
Acquires, stores, presents Credentials
Sends Presentation
Issuer
Creates, issues, and revoke Credentials
Verifiabl e Data Registry
Verifier
Receives and verifies Presentatio ns

What are we working on?

Digital Credentials API

- In this context, **governments have been implementing decentralized identity models for citizens** in recent years, as an improvement from Centralized and Federated models.
- This brings **additional challenges**, if we are on human credentials (in particular issued by governments) , we have **threats to security, privacy, and human rights**.
- Also, **how to use these credentials on the Web**?
- The **Digital Credentials API** has been proposed for **user agents to mediate credentials from a Website to the Wallet.**



Layer 5: Trust Frameworks and Ecosystems

Governance and Trust Frameworks

Layer 4: Applications, Wallets, Products

Website

Wallet

Website

Layer 3: Credentials

Issuer
Issues Credentials

Issues Credentials

VC

Holder
Acquires, stores, presents Credentials

Presents Credentials

VP

Verifier
Verifies Credentials

Layer 2: Agents and Infrastructures

Agent

Register information for verification

Agent

Register Identifiers and use Schemas

Agent

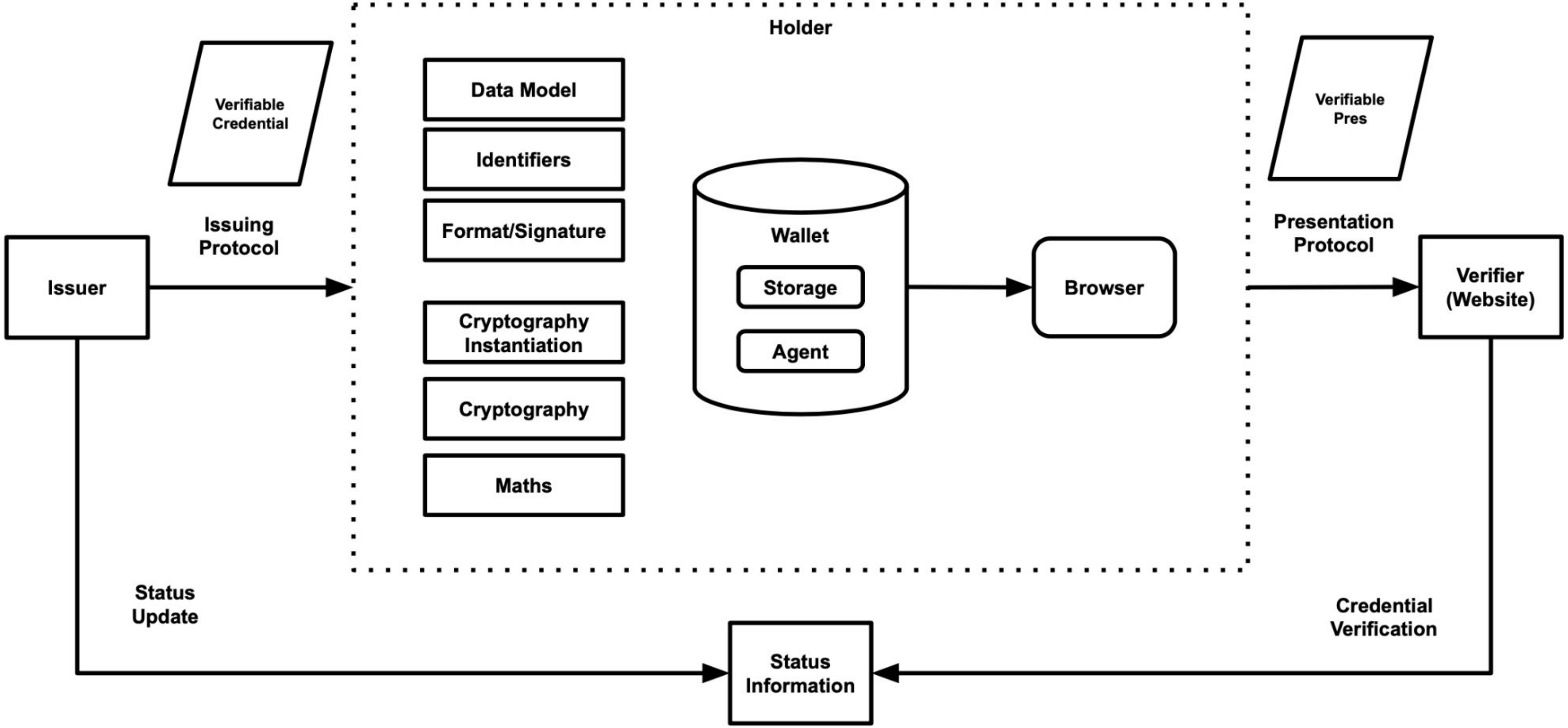
Reads information for verification

Layer 1: Identifiers and Namespace

Identifiers

Verifiable Data Registry
Maintains identifiers, schemas, and relevant information needed for verification

Decentralized Identity Architecture



Layer 3: Credentials, Browser Edition

What can go wrong?

Newly identified threats

- It has been requested to include the Digital Credentials API within the Federated Identity Working Group.
- So a recharter of the group with expanded scope was proposed to the Advisory Committee.
- During the W3C Process for the recharter, a Formal Objection was received, where it is requested to resolve some threats related to the Decentralized Identities.
- The Team has begun mediation with the objector, convening the Council and is preparing the report but, since Threat Modeling is collaborative and we’ve a living Threat Model for Digital Identities, let's see together what are we going to do about it?

What can go wrong?
Introduction

- Aim to separate fundamental concerns from technical merits.
- Objection focuses on broader issues beyond technical aspects.
- Suggest discussing concerns independently:
  a. Perpetuates sharing of personal data by making it more available via a browser API
  b. Increased centralization through subtle tradeoffs
  c. Content will be moved from the deep web to the “attributed deep web”
  d. Exchanges user agency for greater compliance and convenience

What can go wrong?

Perpetuates sharing of personal data by making it more available via a browser API

- **Increased Accessibility of Personal Data:** Introducing a digital credentials API makes personal data more accessible through browsers.
- **Jevons Paradox Effect:** Easier access leads to increased consumption and requests for data.
- **Reduction in User Privacy:** Users may be expected to provide more third-party-attested data.
- **Insufficient Technical Solutions:** Current proposals do not adequately address these privacy concerns

What can go wrong?

Increased Centralization Through Subtle Tradeoffs

- **Digitization of Trust:** Reliance on trusted third-party issuers for credentials centralizes authority.
- **Centralization Similar to Single Sign-On Systems:** Limited number of providers dominate, reducing diversity and increasing dependency.
- **User Control Undermined:** Security measures require trusted operating systems and certified wallets. Users cannot modify or control wallet software, credentials, or keys.
- **Impact on User Agency:** Prioritizes issuers and verifiers over users, undermining control over personal devices and software.

What can go wrong?

Content Shift to the "Attributed Deep Web"

- **Restricted Access to Content:** Sites may require "proof of personhood," limiting openness.
- **Rise of Walled Gardens:** Examples: Social media platforms requiring login or identity verification. Content becomes less accessible to the general public.
- **Exclusion of Undocumented Individuals:** Mandatory proof of identity increases the digital divide.
- **Potential Fracturing of the Web:** Access may become restricted based on nationality or legal status.
- **Chilling Effect on Freedom of Expression:** Users may self-censor due to fear of repercussions.
- **Questioning the Endorsement of This Pattern:** Challenges the principle of an open and inclusive web

What can go wrong?

Exchange of User Agency for Compliance and Convenience

- **Power Imbalance Amplified:** Systems increase control of platforms over users.
- **Decreased User Autonomy:** Trust shifts to third-party issuers chosen by verifiers. Users become subjects rather than active agents.
- **Reduced Control Over Personal Data:** Individuals seen as less authoritative over their data compared to issuers. Example: Misgendering due to unchangeable government-issued credentials.
- **Institution-Driven Systems:** Decisions made for compliance and convenience, not user choice.
- **Limited User Options:** Share attested data or forgo using certain web services.
- **Impact on Core Web Principles:** Accepting the API may undermine user agency, a foundational aspect of the web.

What can go wrong?

Other Threats?

What are we going to do about it?

Threat Modeling - Decentralized Credentials @ TPAC

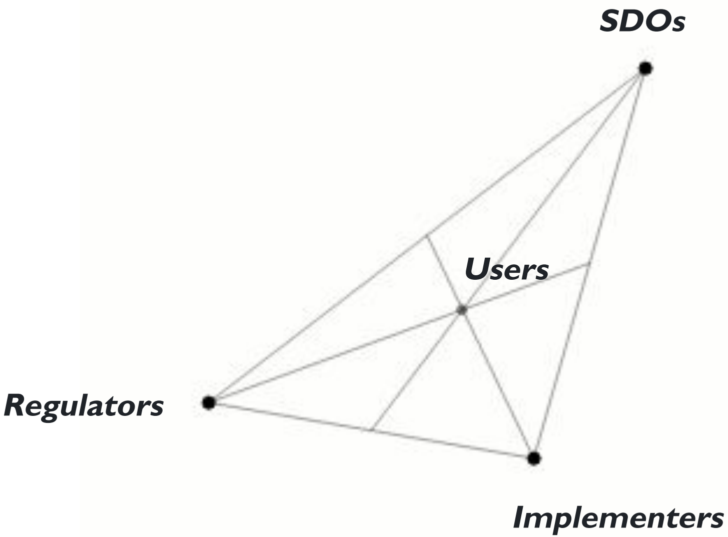
Did we do a good job?

(metaphorical question)

- Join Threat Modeling Community Group (we can continue the discussion after TPAC)
- PR the Threat Model!

Thank you!

The Three Body Problem


SDOs
Users
Regulators
Implementers